ORDER FOR SUPPLIES OR SERVICES (FINAL)

PAGE 1 OF 1

N65236-13-D-4897	0010	2015 Sep 28	N65236-15-NR-55289	DO-A7

6. ISSUED BY CODE N65236

SPAWAR-Systems Center Lant (CHRL)
P.O. BOX 190022
North Charleston SC 29419-9022
Theodore Rivera/22210
843-218-2717

7. ADMINISTERED BY CODE S2404A

DCMA Manassas
14501 George Carter Way
Chantilly VA 20151

8. DELIVERY FOB
□ DESTINATION
□ OTHER
□ *(See Schedule if other)*

9. CONTRACTOR CODE 1QU78 FACILITY

CACI,INC-FEDERAL
14370 Newbrook Dr
CHANTILLY VA 20151

10. DELIVER TO FOB POINT BY *(Date)*
See Schedule

11. X IF BUSINESS IS
□ SMALL
□ SMALL DISADVANTAGED
□ WOMEN-OWNED

12. DISCOUNT TERMS
Net 30 Days
WIDE AREA WORK FLOW

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
See Section G

14. SHIP TO CODE

See Section D

15. PAYMENT WILL BE MADE BY CODE HQ0338

DFAS Columbus Center,South Entitlement Operations
P.O. Box 182264
Columbus OH 43218-2264

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER	DELIVERY/ CALL	X	This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of numbered contract.
	PURCHASE		Reference your furnish the following on terms specified herein.
			ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

CACI,INC-FEDERAL		Carla Rollins Contracts Sr. Manager	
NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED *(YYYYMMDD)*

□ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE
See Schedule

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED *	21. UNIT	22. UNIT PRICE	23. AMOUNT
	See Schedule				

**If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.*

24. UNITED STATES OF AMERICA

BY: /s/Theodore Rivera 09/28/2015
CONTRACTING/ORDERING OFFICER

25. TOTAL $10,059,780.40

26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
□ INSPECTED □ RECEIVED □ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP NO.	29. D.O. VOUCHER NO.	30. INITIALS
	□ PARTIAL □ FINAL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR
f. TELEPHONE / g. E-MAIL ADDRESS	31. PAYMENT □ COMPLETE □ PARTIAL □ FULL		34. CHECK NUMBER
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.			35. BILL OF LADING NO.
a. DATE / b. SIGNATURE AND TITLE OF CERTIFYING OFFICER			

37. RECEIVED AT	38. RECEIVED BY *(Print)*	39. DATE RECEIVED	40. TOTAL CON-TAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

SECTION B SUPPLIES OR SERVICES AND PRICES

CLIN - SUPPLIES OR SERVICES

For Cost Type Items:

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
2001	R425	BFS Support Services - Funding #1 Services to be performed in accordance with the PWS. - CPFF (Fund Type - TBD)	1.0	LO	(b)(4)		$10,059,780.40
200101	R425	Funding Doc #1 (Fund Type - TBD)					
200102	R425	Funding Doc #2 (Fund Type - TBD)					
2006		Contract Data Requirements List (CDRL) in accordance with DD1423,see Exhibit A.					$0.00

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
3001	R425	BFS Support Services - Funding #1 Services to be performed in accordance with the PWS. - CPFF (Fund Type - TBD) Option	1.0	LO	(b)(4)		
3006		Contract Data Requirements List (CDRL) in accordance with DD1423,see Exhibit A.					$0.00

Item	PSC	Supplies/Services	Qty	Unit	Est. Cost	Fixed Fee	CPFF
4001	R425	BFS Support Services - Funding #1 Services to be performed in accordance with the PWS. - CPFF (Fund Type - TBD) Option	1.0	LO	(b)(4)		
4006		Contract Data Requirements List (CDRL) in accordance with DD1423,see Exhibit A.					$0.00

SECTION C DESCRIPTIONS AND SPECIFICATIONS

TASK ORDER (TO) PERFORMANCE WORK STATEMENT (PWS)

SPACE AND NAVAL WARFARE SYSTEMS CENTER, ATLANTIC

SHORT TITLE: NAVFAC CIO IT SUPPORT

1.0 PRIMARY PLACE(S) OF PERFORMANCE

a. Government/Contractor facilities - Washington D.C.

2.0 TASK ORDER PURPOSE

2.1 BACKGROUND

Naval Facilities Engineering Command (NAVFAC) builds and maintains sustainable facilities, delivers utilities and services, and provides Navy expeditionary combat force capabilities. NAVFAC executes this mission via execution within six (6) Business Lines: Capital Improvements, Environmental, Expeditionary, Public Works, Asset Management, and Contingency Engineering. NAVFAC's ability to realize its vision via the Business Lines above is dependent on its ability to better capture, store, analyze, and report on information it generates/collects during the course of executing its mission. Enhancing the ability to visualize information about the efficiency and effectiveness of execution across Business Lines will help reduce operations costs and align operations with its customers' and leadership's expectations.

The scope of work to be performed is focused on delivering high-value business solutions and capabilities to employees, partners, and customers to enable NAVFAC to optimize mission accomplishment. The scope of work will focus on the following: N0002515RC00146-AA-1751804-09/30/2016, N0002515RC00147-AA-1751804-09/30/2016

- Managing, monitoring and improving Information Technology (IT) infrastructure to increase customer trust and satisfaction while continuing to define, develop and build Enterprise Data Warehouse (EDW)
- Providing access and insight to authoritative enterprise information
- Working toward the dedication to standards and governance processes as well as a focus on transparency and openness to ensure end-users are appropriately informed, trained and included in capability delivery
- Implement a standardized, aligned, synchronized and innovative framework within the organization, linking systems, applications, processes and users to empower and manage quantum innovation across the organization
- Leveraging NAVFAC systems and Commander, Naval Installations Command (CNIC) Gateway 2.0 (G2), the team will focus on providing a venue to develop innovative opportunities across the enterprise, in close collaboration across all levels of the organization

NAVFAC Command Information Office (CIO) is responsible for the overall successful implementation of the requirements described in this document. In addition, as part of the CIO's responsibility to NAVFAC, the CIO is called upon to improve IT resource utilization, enhance IT application quality, improve IT user satisfaction, all while supporting NAVFAC's core organizational strategy. NAVFAC CIO will utilize advisory services to support these objectives and to effectively deliver business outcomes and change in the organization.

In an effort to improve government oversight, increase system/application interoperability, and improve cost efficiencies, NAVFAC CIO has requested SPAWAR Systems Center Atlantic to provide technical and programmatic support to implement a number of business/mission – focused IT initiatives. Those IT initiatives are described in the Scope section below.

SPAWAR Systems Center Atlantic will provide technical and program management support of the Enterprise Information Management (EIM) Framework and Solutions, Enterprise Architecture, Gateway 2.0 (G2), Enterprise Content Management (ECM) Strategy and Development, Application/System Modernization, Cyber Security, Information Assurance (IA) and Program Management.

2.2 SCOPE

For this project, SPAWAR Systems Center Atlantic requires contractor support in service of initiatives that share the common goal of using accurate information collected from across the NAVFAC enterprise to visualize information that drives greater visibility of performance and more informed executive decision-making related to execution of initiatives within NAVFAC's 6 Business Lines.

The scope of contractor support will include:

- Enterprise Information Management (EIM) Framework
- EIM Solution Development
- Enterprise Architecture (EA) Development
- G2 Support
- Enterprise Content Management (ECM) Strategy and Governance
- ECM Solution Development
- Application/System Modernization
- Cyber Security
- Program and Project Management

3.0 APPLICABLE DOCUMENTS

3.1 REFERENCES

All references listed within the basic contract are required as applicable to this TO. In addition, the following reference(s) is identified specific to this TO:

	Document Number	Title
a.	NIST 800-66	Health Insurance Portability and Accountability Act (NIST 800-66, Resource Guide for Health Insurance Portability and Accountability Act of 1996 (HIPAA))
b.	NIST 800-53A	Federal Information Management Act (FISMA) of 2002 (NIST 800-53A, Guide for Assessing the Security Controls in Federal Information Systems)
c.	SECNAVINST 5239.3A	Secretary of Navy Instruction (SECNAVINST) 5239.3A, DON Information Assurance Policy
d.	DoDI 8500.1	Department of Defense Instruction (DoDI) 8500.1 Cybersecurity

e.	NIST SP-800-37	National Institute of Standards and Technology (NIST) SP-800-37 Guide for the Security Certification and Accreditation of Federal Information Systems
f.	NIST SP-800-53	NIST SP-800-53 Recommended Security Controls for Federal Information Systems
g.	DCID 6/3	DCID 6/3 Protecting Sensitive Compartmented Information Within Information Systems (DCID 6/3)—Manual
h.	Executive Order 12958	Executive Order 12958, National Security Information, Executive Office of the President, July 1995
i.	National Security Directive 42	National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, Executive Office of the President, July 1990
j.	Office of Management and Budget Circular A-130	Office of Management and Budget Circular A-130, Management of Federal Information Resources, Executive Office of the President, 8 February 96
k.	Public Law 100-235	Public Law 100-235, 101 STAT.1724, Computer Security Act of 1987, 8 January 1988
l.	NSTISS Policy No. 200	National Security Telecommunications and Information Systems Security (NSTISS) Policy No. 200, National Policy on Controlled Access Protection, National Security Telecommunications and Information Systems Security Committee, July 1987
m.	DITSCAP 5200.40	DoD Information Technology Security Certification and Accreditation Process (DITSCAP) 5200.40, 7 October 1999
n.	DoDI 8510.bb	DoDI 8510.bb, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
o.	DoDI 8510.01	Risk Management Framework (RMF) Reissues and renames DoD Instruction (DoDI) 8510.01
p.	DoDI 8500.00	Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
q.	DOD 8570.01M	Department of Defense 8570.01 Manual – Information Assurance Workforce Improvement Program
r.	CJCSI 6510.01F	Information Assurance (IA) and support to Computer Network Defense (CND) 09 Feb 2011

3.2 SPECIFICATIONS

All specifications listed in the basic contract are applicable as required by this TO.

4.0 SECURITY REQUIREMENTS

4.1 ORGANIZATION

As specified in clause 5252.204-9200 and the Contract Security Classification Specification form, DD-254, classified work shall be performed under this task order. The contractor shall have SECRET clearance at time of TO award.

4.2 PERSONNEL

Prior to any labor hours being charged on this TO, the contractor shall ensure their personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access level required for the task order, and if applicable, are certified/ credentialed for the Cybersecurity Workforce (CSWF). All personnel shall possess a SECRET clearance prior to working on TO.

5.0 COR DESIGNATION

The Contracting Officer Representative (COR) for this task order is (b)(6) 58100 who can be reached at; e-mail: (b)(6) @navy.mil.

6.0 DESCRIPTION OF WORK

6.1 ENTERPRISE INFORMATION MANAGEMENT (EIM) FRAMEWORK

NAVFAC CIO acts as a partner with all NAVFAC Business Lines to enable improving operational performance and cost reductions through business process definition, analysis, and development of technical capabilities with automated processes and improved transparency for analytics and decision making. In support of this effort, SPAWAR Systems Center Atlantic requires the development and maintenance of a standard process and framework for (1) how the CIO will interact with NAVFAC Business Lines during the visioning phase of projects and (2) how the CIO will plan, deliver, and sustain solutions developed in partnership with the Business Lines.

The contractor support services in this area shall include:

- Development of a solution implementation lifecycle that incorporates principles of the Enterprise Information Management (EIM) processes and carries a project from ideation through implementation
    - Detail is required on how the proposed solution will scale as many projects (with various Business Lines) are incorporated in parallel
- Development of a Playbook that describes the organizational constructs and management/execution processes that operationalize the EIM Framework and are required to complete an EIM project (CDRL A021). The Playbook that is developed shall:
    - Articulate interactions between contractor and CIO throughout the development process for appropriat check-points to reduce risk
    - Describe interaction between the CIO and Business Line project sponsor throughout the lifecycle
    - Address methodology and interaction with geographically dispersed teams
    - Describe the appropriate project management reporting and structure for all projects executed under th Playbook to include schedule, risk, and financial management
- Define, develop and implement solutions which support NAVFAC's CIO to better document, visualize and understand the products/services, business processes, measurements and authoritative data sources

6.2 ENTERPRISE INFORMATION MANAGEMENT (EIM) SOLUTION DEVELOPMENT

NAVFAC CIO will partner with NAVFAC Business Lines to execute projects which have entered their portfolio through the EIM Framework. The following tasks represent the execution of solution development for projects managed through the EIM Framework and supporting Playbook.

The contractor support services in this area shall include:

- The development of project documentation including high-level requirements, high-level solution design, and necessary assumptions and risks for review by the CIO and Business Line prior to project authorization (CDRL A021)
- Identification of stakeholders for business solutions and the development of supporting communication plans throughout the solution development process
- Identification and documentation of functional requirements for the proposed solution
- Execution of the software development life cycle to design, develop, test and deploy the solutions.

Solutions shall include:

  - Custom application development
  - Customization of Microsoft SharePoint or Oracle WebCenter and the development of web parts as necessary
  - Business Intelligence and Advanced Analytical Solutions
  - Automated Forms Management
  - Geospatial Analytical Solutions

- In addition to the development of business solutions, the contractor shall be responsible for the architecture, development, and maintenance of NAVFAC's EDW including:
  - EDW Conceptual Design and Architecture
  - EDW Roadmap and Strategy
  - Master Data Management Plan and execution of approved plan
  - Integration of NAVFAC, DoN, DoD, and non-DoD data sources into the EDW
  - Creation of transactional history where applicable
  - Design and development of Extract, Transform, and Load (ETL) jobs to support EDW build-out and EI solutions
  - The development of dimensionalized data models in support of analytical solutions
  - The development and execution of NAVFAC's Data Governance Plan including:
    - Establishment of Data Stewards
    - Maintenance of a Data Dictionary
    - Facilitating Meetings of the Data Governance Council
  - The development and execution of NAVFAC's Data Quality Plan including:
    - Data profiling to find data quality issues/concerns
    - Implementing data quality transformations
    - Establishment of a methodology to allow users to easily understand data lineage and latency whei EIM solutions
    - Regular program management reporting on data quality issues
- Development and deployment of the appropriate training and communications plans to enable users to use deployed functionality (CDRL A021)

6.3 ENTERPRISE ARCHITECTURE (EA) DEVELOPMENT

NAVFAC CIO is implementing an Enterprise Architecture (EA) initiative to streamline and optimize NAVFAC's IT portfolio for improved support of NAVFAC's mission. EA is a structured, repeatable mechanism to help NAVFAC deliver greater value by explicitly linking business and IT capabilities to the organization's overall strategy and mission. Creating a well-defined and understood EA for NAVFAC will lead to lower development and maintenance costs while delivering greater value to end users through improved operability and a reduced need for training.

The contractor support services in this area shall include:

- Assessing existing architectural standards in place among NAVFAC's current IT investments
- Performing a gap analysis between the current "As-Is" NAVFAC architecture, and related architectural standards, and the Target EA
- Developing a Target EA for NAVFAC (CDRL A021) based on the current architectural environment and

industry best practices that:

- o Describes both functionally and technically the information management services to be provided by the EIM functional and technical supporting infrastructure
- o Describes connections and communications between services internal to NAVFAC and between the NAVFAC enterprise architecture and external services and data sources
- o Identifies best practices and standards for future state systems developed as part of the NAVFAC IT portfolio
- o Guides and constrains development of individual solutions such that individually developed solutions can compared (referenced against) the EA to ensure use of NAVFAC/Navy-approved tools and services

- Developing a Target State Roadmap, which will lay out EA execution priorities over a defined time period (CDRL A021)
- Continued build out of NAVFAC's SEMOSS EA repository to enable EA analysis and scenario planning

6.4 GATEWAY 2.0 (G2) SUPPORT

NAVFAC seeks to integrate with CNIC G2 business platform to support EIM and other IT initiatives.

The contractor support services in this area shall include:

- Development of technical requirement documentation to support G2 integration functional requirements (CDRL A021)
- Participate, adhere to, and fully integrate with EA Governance, the CNIC enterprise and application management control boards
- Manage all aspects of technical support related to application deployment, modification, installation and business solution integration of G2
- Develop, deploy and operate, and administer standard procedures to manage G2 solution performance and measurements in order to proactively ensure G2 solution availability, reliability, and responsiveness
- Configuration, installation and entry of new systems and services in accordance with CNIC Enterprise Architecture guidance and CNIC and NAVFAC leadership direction
- Configuration of software within CNIC's G2 platform environments
- Perform design and development activities for SharePoint (2007, 2013) , COGNOS Business Intelligence Suite, ESRI ArcServe, MS SCOM, and Microsoft Identity Lifecycle Manager / Microsoft ForeFront, Google Search Appliance
- Manage, support and secure all existing applications and environments
- Strictly adhere to agreed-upon level of service for any operation, administration, additions or changes to the overall infrastructure; propose changes where appropriate for government approval
- Comply with the approved architectures, programs, standards and guidelines
- Perform, as required, weekly/monthly/quarterly IA reviews, in coordination with Navy IT System security policies
- Create technical training material for applications and business solutions for knowledge transfer to the NAVFAC Enterprise Support Center, and other NAVFAC staff designated by the government (CDRL A021)
- Provide installation and configuration information to the hosting staff
- Implement the knowledge transfer and training plan to sustain system administration and operations

- Attend organizational impact planning meetings and implement specified changes
- Participate, adhere to, and fully integrate with EA governance, the NAVFAC enterprise and application management control boards
- Manage all aspects of technical support related to application deployment, modification, installation and business solution integration
- Setup configuration and management of all physical servers including break fix and routine maintenance support
- Perform configuration and management of all switches, routers and firewalls within the hosting centers to include all fiber switches, as necessary
- Perform all required network cabling and wiring of power to support operations

6.5 ENTERPRISE CONTENT MANAGEMENT (ECM) STRATEGY AND GOVERNANCE

NAVFAC's operations generate a sizeable volume of data that could be, but presently is not, sufficiently transformed into usable information to be leveraged by decision-makers at all levels of the chain of command. To transform more of that data into useful information, NAVFAC intends to create an Enterprise Content Management (ECM) system and supporting processes and organizational structures. To deliver these solutions, a current-state ECM assessment and a future-state ECM strategy must be conducted that clearly articulates how NAVFAC's Business Lines and CIO organization will be organized from an ECM role and function perspective, and how NAVFAC would leverage an ECM solution to improve management of content generated across the NAVFAC enterprise. SPAWAR Systems Center Atlantic requires contractor support to create that ECM strategy.

The contractor support services in this area shall include:

- Conducting a current-state ECM assessment that evaluates what content is managed across the enterprise, how it is managed, and how NAVFAC is organized to perform ECM activities
- Executing a Gap Analysis that identifies opportunities for improving NAVFAC's current approach to ECM activities and that recommends specific changes to be made to organizations, processes, and solutions to improve NAVFAC's approach to ECM
- Developing of an ECM strategy focused on determining optimal content management structures, processes, roles, and responsibilities for NAVFAC to address internal-facing and external-facing content management requirements
- Developing a target ECM functional architecture that includes the elements of organization, rule set, management processes, and roles/responsibilities enabling NAVFAC to manage internal business management content and external public affairs content

6.6 ENTERPRISE CONTENT MANAGEMENT (ECM) SOLUTIONS DEVELOPMENT & SUPPORT

Once NAVFAC's new ECM strategy and target functional architecture have been defined and executed, NAVFAC intends to implement several ECM technology solutions to improve its management and delivery of structured and unstructured content both internally and to web audiences. These solutions may include document management solutions, records management solutions, collaboration solutions, web content management solutions, and the like.

The contractor support services in this area shall include:

- Defining detailed ECM solutions based on customer-provided functional requirements and derived technical requirements

- Conducting, for each solution, an Analysis Of Alternatives (AoA) to be used by NAVFAC to evaluate and select products appropriate to each ECM solution type
- Designing, developing, testing, and deploying content taxonomies, structures, templates, and components
- Designing, developing, testing, and deploying ECM solutions possibly including document management solutions, records management solutions, collaboration solutions, and web content management solutions
- Develop or enhance governance/business rules to provide optimized expanded content management, user interface design (due to expansion of capabilities) and support and training for Enterprise Business Solutions (EBS) end users
- Identify new pages and updated navigation necessary to accommodate expanded release requirements
- Update WebCenter portal design and taxonomy for new content and applications. Identify if enhancements or new pages are required for content and applications being developed during each release cycle. Develop and deploy updates as recommended and approved by the government
- Identify any changes necessary to the content authoring, review, publication/ expiration processes, roles and responsibilities based on each new release. Update and implement the Information Management Plan based on the expanded release requirements
- Provide support services to users using the CNIC/NAVFAC Web Content Management (WCM) system
- Designing and developing new features via Adobe CQ for the current WCM system
- Provide WCM engineering support with regard to Amazon Web Service (AWS) deployment & migration

6.7 APPLICATIONS / SYSTEM MODERNIZATION

NAVFAC seeks to modernize operations of its current "siloed" applications and systems, which include multiple custom applications, developed using disparate technologies and platforms. In addition, these applications are supported by offline workarounds requiring manual intervention. Requirements in this area will support the modernization and integration of the business and mission functions currently performed by these siloed legacy systems and offline processes.

The contractor support services in this area shall include:

- Evaluating each application/system targeted for modernization to determine whether it should be upgraded or replaced, and recommending a disposition for each application/system to NAVFAC
- Identifying opportunities for consolidating the application/system footprint to reduce redundancy between legacy applications/systems
- Validation of functional requirements for application/system upgrades/replacements
- Generating system design documentation covering computing infrastructure, facilities infrastructure, capability delivery, and capacity
- Conducting capabilities and limitations (CAP/LIM) assessments, risk assessment, and operational utility assessments to accelerate cost/schedule/performance, to validate target architecture performance, and to assess operational/mission environment functions prior to production deployment
- Performing application/system development activities, including application configuration and custom coding as necessary
- Performing test activities including test planning, test execution, modeling and simulation, and test reporting
- Deploying the validated solution to the NAVFAC production environment in accordance with established NAVFAC configuration methodologies

- Providing a Transition-Out Plan to the Government COR, supporting technology, equipment, documentation, analysis, and cost transition to the production NAVFAC government network managed environment for O&M (CDRL A021)

6.7.1 FACILITIES INFORMATION SYSTEMS (FIS) MODERNIZATION SUPPORT

NAVFAC has developed FIS to provide a single system for management of core financial and facilities information flows in support of General Fund mission execution. FIS interfaces with accounting, real property, contract management, acquisition, and other systems to insure timely and accurate execution of NAVFAC mission objectives. The FIS infrastructure consists of a mix of transactional and batch processes running in a mainframe environment using a mix of JCL, COBOL, and CA-IDEAL with DATACOM as the underlying data repository. System hosting and maintenance of the infrastructure are supported by Defense Information Systems Agency (DISA) and system support, code management, reporting, requirements, and other CDA functions are executed within NITC. Given the strong reliance on requirements documentation in the decision-making process and the necessity to validate requirements for any new or redeveloped solution, a full review of requirements and the disposition of FIS will need to be conducted and an analysis of alternatives developed. Any technology decision must be acceptable to all stakeholders including CIO, CNO, FM, and user representatives. Financial Improvement Program/Financial Improvement and Audit Readiness (FIP/FIAR) and other audit impacts could add to requirements as outside NAVFAC mandates and drivers.

The contractor support services in this area shall include:

- Provide support for analysis of all existing requirements and capabilities
- Review of all existing requirements documentation
- Review of existing capabilities
- Validation of the results with technical and program representatives at Navy Instructor Training Course (NITC), Ech II and Ech III
- Consolidate all validated requirements and deliverables into a single requirements repository

6.8 CYBER SECURITY (CS)

6.8.1 Information Security and Privacy (IS&P) Program / Portfolio Management Support

The contractor support services in this area shall include:

- Developing, tracking and delivering comprehensive schedule information
- Tracking issuances through the designated workflow
- Providing support for Chief Information Officer meetings such as agenda, action items, and meeting minutes
- Reviewing and tracking funding requests
- Participating in the development of Portfolio Management Process which includes development of systems lists, Meeting with Portfolio Manager concerning current and future state of the Portfolio, as well as providing support for the day-to-day management of the programs portfolio
- Identifying system overlap in Portfolio
- Meeting with potential new system owners to review Portfolio Management Process
- Participating in the development of a Portfolio Management Tool
- Updating appropriate IS&P Portfolio Management Issuances
- Providing guidance for systems related to the Portfolio Management process

- Developing Portfolio Management tracking tool
- Training on usage of Portfolio Management tracking tool
- Implement and execute usage of Portfolio Management tracking tool

6.8.2 Certification and Accreditation (C&A) of NAVFAC Information Technology (IT)

The contractor support services in this area shall include:

- Compliance with the most recent DoD 8510 and NIST SP 800 Series Directives and Processes
- Support C&A Program Efforts with stakeholders
  - Review updates of the Defense Information Assurance Certification and Accreditation Process / Risk Management Framework (DIACAP/RMF) artifacts from the system owner and track status of changes
  - Assist in the development of the path to complete accreditation
  - Assemble the DIACAP/RMF Risk Assessment Package IAW DoD 8510 and NIST 800 Series
  - Deliver the DIACAP/RMF Package to the Certifying Authority (CA) in a trusted manner consistent with Department o Defense, Department of Navy, NAVFAC and/or Program requirements
  - Provide C&A support in the areas of operating systems, application security, network/perimeter/wireless, cross domain solutions, Host Based Security System (HBSS), policy and SCAP content, DoD cloud computing security, and mol security requirements
  - Periodically assess Plan of Actions & Milestones (POA&M) scheduling and completeness status and report as required
  - Track assigned system from initiation to retirement, staying informed of Independent Verification & Validation (IV&V)/Security Controls Assessment (SCA) milestones and DIACAP/RMF POA&M deadlines
  - Address accreditation questions from the Program Management Office (PMO)
  - Maintain accreditation schedules for systems
  - Work with the PMO to ensure the correct C&A process is being followed
  - Adhere to certification guidance received from the CA and perform actions necessary to complete certification
  - Participate in all test execution and planning activities, including meetings and working groups, as required
  - Participate in DIACAP/RMF team meetings and system review related meetings to provide technical and non-technical guidance
  - Identify and elevate the need for any additional IA requirements test events needed to support accreditation (includes scheduling of annual reviews)
- Cyber Security Validation Readiness Review
  - Review IA self-assessment results
  - Evaluate IA self-assessment results and evidence during Readiness Review to determine if the security is sufficiently ma to execute an IA certification test event
  - Assist in the determination of IA test level of effort for each planned system
  - Participate in all test execution and planning activities, including meetings and working groups
  - Review DIACAP/RMF documentation prior to Independent Verification and Validation (IV&V) to determine security readiness of system, site, or enclave
- Independent Verification and Validation (IV&V)/Security Controls Assessment (SCA)
  - Support the IV&V/SCA testing of each system, site, or enclave under the CA and Designated Approving Authority/Authorizing Official (DAA/AO) purview
  - Participate in all test execution and planning activities, including meetings and working groups
  - Review all C&A / Assessment and Authorization (A&A) documentation to ensure the information is current, accurate,

applicable to the article of test

- To support standardization, ensure that all IA test procedures are up to date with all current applicable requirements anc that those methods of testing are widely visible and available for NAVFAC to apply to all necessary systems across it enterprise
- Produce individualized IA test procedures for inclusion in the Test Plan that describe how to perform validation actions outlined in the applicable Security Technical Implementation Guide (STIG) checklists
- Analyze previous IA/Cyber Security testing artifacts to tailor IA/Cyber Security tests
- Develop IV&V/SCA Test Plan, provide to system owner, documentation team, and IV&V/SCA team
- Oversee the execution of IA certification testing to identify all vulnerabilities, and document residual risks by conductir thorough risk assessments
- Provide the IA risk analysis and mitigation determination results for use in the test report
- Assist in the development/utilization of automated tools for the creation of necessary test evidence, risk assessment, anc certification artifacts for each system
- Perform wireless discovery using approved DoD software
- Perform application dynamic web services testing using approved DoD tools (e.g. HP WebInspect)
- Perform, on custom code, static source code analysis using approved DoD tools (e.g. HP Fortify)
- Perform, on custom code, software supply chain management verification using approved DoD tools or perform manual
- Perform penetration testing, when necessary, utilizing DoD approved software and tools
- Perform testing with tools to manage the test procedures and results
- Validator and IV&V Representatives to review DIACAP/RMF documentation prior to IV&V
- Schedule IV&V events and assign IV&V team members to meet the requirements of the IV&V test plan
- Provide status report to the COR on progress/results of IA testing
- Identify and elevate the need for any additional IA test events needed to support accreditation (Includes scheduling of an reviews)
- Coordinate test planning identified from IA Validation Team with the CA

- Oversight of POA&M and DIACAP/RMF Scorecard creation
  - Oversee completion of DIACAP/RMF Scorecard
  - Provide Mitigation and Remediation in support of the C&A/A&A process both remotely and on-site
  - Provide POA&M resolution recommendations to meet DoD and Federal technical and operational requirements and guidelines
  - Provide assistance to sites to update outstanding actions contained in the POA&M and requesting extensions for expiri IATOs as required
- Validator
  - Maintain qualified validator status with Navy or other applicable DoN/NAVFAC agency requirement
  - Review all packages before being delivered to CA
  - Work directly with the CA as a qualified agent to ensure validation activities are compliant with the IA/CS test strateg
  - Conduct in-depth analysis of IV&V/SCA, C&A/A&A, and functional/operational test results for accuracy, compliance, adherence to DoD and Federal IA technical and operational security requirements
  - Identify and elevate the need for any additional IA/CS test events needed to support accreditation (Includes scheduling c annual reviews)
  - Work with the system owner to develop specific site or system mitigation plans to achieve an overall reduction in resid risk

- Coordinates with the CA for issuance of a certification recommendation

- Risk Assessments
  - Provide Mitigation and Remediation in support of the C&A/A&A process remotely and/or on-site as required
  - Provide Mitigation and Remediation reports as required(CDRL A021)
  - Conduct in-depth analysis of IV&V/SCA, C&A/A&A,, and functional/operational test results for accuracy, compliance, adherence to DoD and Federal IA technical and operational security requirements
  - Document residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth an provide the IA risk analysis and mitigation determination results for the Test Report
  - Assist the CA and Validator with producing the risk assessment artifacts describing residual risks identified during certification testing

6.8.3 Enterprise Mission Assurance Support Service (eMASS) and Vulnerability Management System (VMS)

The contractor support services in this area shall include:

- eMASS
  - Provide how-to guides and support efficient use of the eMASS system
  - Schedule eMASS training for NAVFAC personnel
  - Provide high level eMASS training and training documentation to new members of Staff (CDRL A021)
  - Assist in the development of the eMASS process flow documents
  - Serve as Tier 1 support to address process issues that are identified in eMASS. Elevate and track software issues to DI through the DISA Enterprise Help Desk.
  - Maintain all applicable NAVFAC Program eMASS user accounts
  - Assist NAVFAC user community with DIACAP/RMF lifecycle for system in eMASS (i.e. System registration, assign DIACAP/RMF team members, control assessment and validation, uploading artifacts, submitting packages and runni applicable reports)
  - Establish and manage inheritance for NAVFAC Enterprise
  - Create/run system reports and create organizational metrics to report to leadership team (CDRL A021)
- VMS, Online Compliance Reporting System (OCRS), Vulnerability Remediation Asset Manager (VRAM)
  - Provide "How-to-Guides" to support efficient use
  - Schedule VMS, OCRS, VRAM, and Assured Compliance Assessment Solution (ACAS) training for NAVFAC Person
  - Provide training to new staff along with training documentation (CDRL A021)
  - Assist in the development of the VMS, OCRS, VRAM Process Flow
  - Serve as Tier 1 support to address issues that are identified in VMS. Elevate and track software issues to DISA throug the DISA Enterprise Help Desk.
  - Assist NAVFAC user community with DIACAP/RMF lifecycle for system in VMS, OCRS, VRAM (i.e. System registration, assigning DIACAP/RMF team members, control assessment and validation, uploading artifacts, submitt packages and running applicable reports)
  - Establish and manage inheritance for NAVFAC Enterprise
  - Create/run system reports and create organizational metrics to report to leadership team
  - Maintain all applicable NAVFAC Program VMS, OCRS, VRAM user accounts

6.8.4 Information Assurance (IA) Officer / Information System Security Officer

The contractor support services in this area shall include:

- Ensure that all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their IA responsibilities before they are granted access to the DoD information system
- Initiate protective or corrective measures when an IA incident or vulnerability is discovered
- Ensure that IA and IA-enabled software, hardware, and firmware comply with appropriate security configuration guidelines
- Ensure that DoD information system recovery processes are monitored and that IA features and procedures are properly restored
- Ensure that all DoD information system IA- related documentation is current and accessible to authorized individual
- Implement and assist in the enforcement of all DoD information system IA policies and procedures, as defined by its security certification and accreditation documentation
- Advise appropriate senior leadership or authorizing official of charges affecting the organization's IA posture
- Collect and maintain data needed to meet system IA reporting
- Ensure that IA inspections, tests, and reviews are coordinated for the network environment
- Ensure that IA requirements are integrated into the continuity planning for that system and/or organization(s)
- Ensure that protection and detection capabilities are acquired or developed using the Information system security engineering approach and are consistent with organization-level IA architecture
- Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed
- Evaluate cost-benefit, economic, and risk analysis in decision-making process
- Participate in information security risk assessment during the Security Assessment and Authorization (SA&A) process
- Participate in the development or modification of the computer environment IA security program plans and requirements
- Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations
- Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents
- Recognize a possible security violation and take appropriate action to report the incident, as required
- Recommend resource allocations required to securely operate and maintain an organization's IA requirements
- Supervise or manage protective or corrective measures when an IA incident or vulnerability is discovered
- Use federal and organization-specific published documents to manage operations of their computing environment system(s)
- Identify security requirements specific to an IT system in all phases of the system lifecycle
- Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
- Assure successful implementation and functionality of security requirements and appropriate IT policies

and procedures consistent with the organization's mission and goals

- Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed; compliance monitoring occurs)
- Participate in the acquisition process as necessary, following appropriate supply chain risk management practices
- Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate

6.8.5 Certification and Accreditation (C&A) / Assessment and Authorization (A&A) Documentation and Policy Support

The contractor support services in this area shall include:

- Develop all C&A documentation in accordance with DoD policies, NAVFAC policies and procedures to ensure that accreditation packages are complete and system compliance is met for Designated Accrediting Authority
- Maintain documentation Plan of Action and Milestones
- Develop C&A documentation to ensure the information is current, accurate, and applicable to the article of test
- Develop IA self-assessment results and evidence during Information Assurance Validation Readiness Review (IAVRR) to determine if the system security is sufficiently mature to execute the IA certification test event
- Participate in DIACAP Team Meetings
- Utilize Enterprise eMASS and VMS for the documentation of test evidence and risk assessment for each system
- Develop Documentation and other required artifacts required for C&A Packages
- Develop associated DIACAP IA Artifacts to include the System Security Plan, System Design and Architecture, Contingency Plan/COOP Plan, Incident Response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote Access artifacts
- Analyze organizational information security policy
- Assess policy needs and collaborate with stakeholders to develop policies to govern IT activities
- Define current and future business environments
- Design a cybersecurity strategy that outlines the vision, mission, and goals that align with the organization's strategic plan
- Develop and maintain strategic plans
- Assist in the development of policy, programs, and guidelines for implementation.
- Assist in the drafting and publishing of security policy for government review and acceptance
- Establish and maintain communication channels with stakeholders
- Identify and address IT workforce planning and management issues, such as recruitment, retention, and training
- Identify organizational policy stakeholders
- Monitor the rigorous application of information security/IA policies, principles, and practices in the delivery of planning and management services

- Obtain consensus on proposed policy change from stakeholders
- Provide policy guidance to IT management, staff, and users
- Review existing and proposed policies with stakeholders
- Support the Chief Information Officer in the formulation of IT-related policies.
- Write information assurance (IA) instructions.
- Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
- Ensure established cybersecurity strategy is intrinsically linked to organizational mission objectives.
- Draft and publish a supply chain security and risk management policy.
- Identify and track the status of protected information assets.
- Apply knowledge of assessment data of identified threats to decision-making processes.
- Translate applicable laws, statutes, and regulatory documents and integrate into policy.
- Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.
- Assist in the Development and maintain agency level cyber security policy and processes that implements DoD Cyber Security program
- Assist in the Development and maintain agency level cyber security policies and processes
- Assist in the Development and maintain agency level RMF policy
- Provide training, reporting, guidance and support to meet the requirements of the DoD IA Workforce Improvement Program Provide guidance on recommended contracting language for built in security for IT solutions
- Ensures enterprise-wide compliance reporting is standardized across NAVFAC and meets DoD cyber security policy requirements

6.8.6 Information Assurance Self Assessments

The contractor support services in this area shall include:

- Preparations:
  - Work with IV&V Lead from NAVFAC to develop Test Plan
  - Participate in System related meetings
  - Prepare for onsite self-assessment
- Self-Assessment Execution:
  - Execute tests per the Test Plan
  - Prepare test events status reports and out briefs (CDRL A021)
  - Populate Validator database/VMS/eMASS with test results
  - Contribute to Test Event Reporting
  - Assemble DIACAP Package (DIACAP Scorecard, POA&M, certification documentation, and system-provided System Identification Profiles (SIP) & DIACAP Implementation Plans)
- Develop plans to validation actions as outlined in the applicable Security Technical Implementation Guide (STIG) checklists
- Validate DIACAP Implementation Plan (DIP) and/or System Security Plan (SSP)

- Assist IA Analyst / Test Team Lead with evaluating IA self-assessment results and evidence
- Participate in Cyber Security Risk Management team meetings
- Ensure IA test procedures are available and visible for use of replication across system using the same software
- Utilize eMASS, VMS, OCRS, VRAM or any required system for the documentation of test evidence and risk assessment for each System

6.8.7 Monitor and Coordinate

The contractor support services in this area shall include:

- Monitor assess Federal Law and Executive Agency Policy / Publications for impact to NAVFAC Cyber Security program
- Cyber Security Coordination – External/Internal policy/compliance
- Assist NAVFAC liaison to DoD, and other overarching policy/direction entities
- Reviews published/emerging DoD Cyber Security policy for incorporation into NAVFAC policy
- Reviews for compliance with DoD and NAVFAC policy enterprise-wide cyber security business processes in support of the information technology acquisition life cycle
- Review and analyze existing/emerging IA policies across services / agencies that are consolidated under NAVFAC structure

6.8.8 System Guidance

The contractor support services in this area shall include:

- Governance
- Perform system assessments with a focus on IA/CS policy
- Review system documentation and coordinate with system owners to gather information in support of IA/CS assessment
- Determine possible options for system certification and accreditation
- Provide recommended option for system certification and accreditation
- Identify IA/CS concerns and risks
- Provide estimated IA cost for system lifecycle
- Perform desktop application IA assessments

6.8.9 IT Contingency Planning

The contractor support services in this area shall include:

- Provide guidance and support related to IT Contingency Planning (ITCP)
- Develop templates in support of ITCP
- Assist in the development and maintain procedures related to tabletop exercises for contingency plans, as well as develop scenarios
- Support execution of tabletop exercises for NAVFAC community
- Participating in the tabletop exercise
- Provide summary of scenario outcomes and recommended changes to specific ITCP plan being reviewed

6.8.10 Information Assurance Managers (IAM)/Information Security System Manager (ISSM) Program

The contractor support services in this area shall include:

- Assist in the Development of a NAVFAC Information Assurance Manager/Information System Security Manager

Program

- Provide policy and process support to NAVFAC IAM/ISSM Community
- Assist in the Development of policies and processes to support policy exception requests to IAM/ISSM Program

6.8.11 Functional Systems Support for Cyber Security

The contractor support services in this area shall include:

- Utilize (IA) Tools (including but not limited to – Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), System Center Configuration Manager (SCCM), Data at Rest (DAR), Data in Transit, Group Policy Objects (GPO), Central Logging and audit reduction analysis)
- Support the use of complementary scanning and patching tools as necessary to maintain sites' security postures
- Review ACAS deployment to support site administrators ability to scan all confirmed assets with an all audits scan (or equivalent) in accordance with local, Navy, or DoD scanning policies
- Provides policy support and oversight for IA Tools (including but not limited to – ACAS, HBSS, SCCM, DAR, GPO, and Central Logging)
- Provide remote and onsite surge support to the networking team and sites for system and network based situations that negatively impact technical security posture
- Define, govern, and manage changes to the baseline configurations and technical policy of all technical tools in the operational environments
- Review HBSS deployment to ensure site assets are adequately protected and properly managed
- Provide technical recommendations and support for security related events of interest, including on site incident response activities
- Provide periodic knowledge transfer regarding the use and configuration of IA/CS tools from surge support to the stakeholder community

6.8.12 Enterprise Cyber Security Compliance

The contractor support services in this area shall include:

- Provide enterprise notification of compliance activities (e.g., Communications Tasking Order (CTO) requirements) that impact enterprise services to and/or within a site of service and/or Program of Record (POR)
- Provide oversight and compliance reporting for the Information Assurance Vulnerability Management (IAVM) program.
- Provide regular status reporting for IA Vulnerability notifications compliance status within and across the Enterprise
- Stay abreast of IA Vulnerability notifications
- Maintain and provide IAVM templates for use in C&A/A&A process to enclave Information Assurance Managers (IAM)/ISSM and POR Program Managers (PM)
- Keep leadership informed of IA Vulnerability notifications impacting service capabilities via e-mail and/or Report of the Day (ROD) notifications
- Provide IAVM notification metrics on a weekly basis
- Provide IA vulnerability (e.g., CTO and Information Assurance Vulnerability Alert/Bulletin) status reports on an as needed basis(CDRL A021)
- Provide compliance templates (e.g. IAVM plans and mitigation plans) on an as needed basis

6.8.13 Incident Response and Analysis

The contractor support services in this area shall include:

- Provide technical recommendations and support for Enterprise Cyber Incident Response and Analysis teams, including on-site incident response activities

- Continuously monitor (24x7) all centrally managed assets (e.g. Nitro, Riverbed, PORs) and analyze possible cyber security events, intrusions, and anomalies impacting site and centrally controlled assets, as detected by Enterprise-managed IA tools, to include, the Nitro Security Event Information Manager, Active Directory (AD) servers, HBSS servers, and network-based Intrusion Protection System (IPS)
- Analyze cyber security events, intrusions, anomalies, and events using network and host-based tools, Nitro Security Information Event Manager (SIEM), network-based IPS, and other supporting tools
- Notify, when necessary, site IAMs of detected events impacting their areas of responsibility
- Serve as central point of contact to the NAVFAC Information Security Division Computer Network Defense Service Provider (CNDSP) for all reported cyber incidents on NAVFAC networks
- Respond to and investigate cyber incidents of interest
- Maintain, execute, and update the NAVFAC Enterprise Incident Response Standard Operating Procedures and Plan on an as-needed basis (required yearly)
- Provide enterprise-wide cyber incident metrics and threat analyses to NAVFAC
- Liaison, as necessary, with surge support to develop recommendations for technical policy changes (IPS Blocks, DNS domain naming service (DNS) Blackholes, etc.) to NAVFAC Information Security Office in response to detected threats and other emerging changes in the cyber landscape as detected by the NAVFAC CNDSP and cyber security stakeholders and contractor

6.8.14 Continuous Risk Management

The contractor support services in this area shall include:

- Update and modify the common risk impact criteria in the form of Risk Management Framework (RMF) on centralized location
- Develop, maintain, and update a baseline risk assessment of the NAVFAC Enterprise
- Execute business plan assessments for NAVFAC enclaves
- Provide regular risk assessment reports to NAVFAC Information Security Division Chief via the RMF (CDRL A021)
- Provide risk mitigation strategies and recommendations to NAVFAC Information Security Division Chief in after-action reports and/or quarterly reports reflecting trends and issues across the Enterprise (CDRL A021)
- Provide IA policy support and guidance for cross functional NAVFAC enterprise cyber security support
- Review new or updated Federal, DoD, and DoN policy and directives, providing feedback to authors and/or appropriate NAVFAC stakeholders as necessary

6.8.15 Cyber Security Workforce (CSWF) Report

The contractor support services in this area shall include:

- CSWF Reports (CDRL A003) shall be developed, maintained, and submitted monthly. If IA/CS support is provided, the contractor shall provide a CSWF list that identifies those individuals who are IA/CS trained, certified and meet requirements for DoD and DoN.

6.9 PROGRAM AND PROJECT MANAGEMENT

SPAWAR Systems Center Atlantic requires project management in support of the breadth and depth of scope described throughout this PWS. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS.

The contractor support services in this area shall include:

- Establishing processes to govern the other tasks in this document, including risk management, schedule management, cost management, and quality management

- Scheduling, coordinating, and hosting a project kick-off meeting at the location approved by the Government
- Delivering weekly and monthly status reports that provide programmatic and financial updates to SPAWAR System Center Atlantic that include: (CDRL A002)
  - Status of current and planned tasks and subtasks
  - Base schedule overlaid with actual schedules, for each task
  - Project Organization
  - Project Transition Processes and Schedule
  - Work Breakdown Structure (WBS)
  - Overall Organizational Structure
  - Task dependencies and interrelationships
  - Contractor personnel assignments and duration (Staffing Plan)
  - Updated Deliverable Schedule (based on solution)
  - Contractor travel information
- Prepare and conduct routine project review meetings
- Manage schedules, milestones and cost
- Establish and implement risk and issue management process
- Review schedule, milestones, budget, risks, and deliverable with SPAWAR Systems Center Atlantic, NAVFAC CIO and Business Line sponsors
- Program and task order specific metrics reporting in various sponsor and task formats as required
- Program and task order specific financial reporting in various sponsor and task formats as required
- Provide Inventory Tracking Report (CDRL A011)
- Provide Contract Funds Status Report (CFSR) (CDRL A018)
- Provide Quality Documentation (CDRL A007) as required
- Provide Wide Area Work Flow (WAWF) invoicing notification and support documentation (CDRL A016)
- Provide Invoice Support Documentation (CDRL A016)
- Provide status report to the COR on progress/results of IA testing
- Support and provide minutes and status reports for collaborative meetings
- Providing IA oversight, project management, and logistics for the task
- Provide project management, planning, and coordination for task order requirements
- Work with the COR to ensure project management and reporting templates are defined and maintained for all new drafts
- Assist in Navy Marine Corps Intranet (NMCI) Customer Technical Representative (CTR) support to include purchase requests for IT assets.
- Develop reports utilizing applications such as: Microsoft SharePoint, Access, or Excel

The contractor shall provide CIO advisory support. The contractor support services in this area shall include:

- Supporting IT strategy and planning by integrating business and IT processes, allowing for continuous assessment and adjustments in response to new opportunities and changing operational conditions;

- Advising NAVFAC on IT transformation to reshape IT operations and organization to better support NAVFAC's mission;
- Advising NAVFAC on IT strengths and risks across a wide array of IT disciplines;
- Supporting NAVFAC IT value management by formalizing the tools and processes needed to drive greater value from IT portfolio investments

6.10 TASK ORDER ADMINISTRATION

In accordance with the basic contract PWS and the requirements of this task order PWS, the contractor shall develop and submit documentation (see CDRL under Para 12.1.1) as required for TO administration.

7.0 GOVERNMENT FURNISHED INFORMATION (GFI)

No GFI will be provided on this TO.

8.0 GOVERNMENT FURNISHED PROPERTY (GFP)

8.1 GOVERNMENT FURNISHED EQUIPMENT (GFE)

No GFE will be provided on this TO.

8.2 GOVERNMENT FURNISHED MATERIAL (GFM)

No GFM will be provided on this TO.

9.0 CONTRACTOR ACQUIRED PROPERTY (CAP)

9.1 CONTRACTOR ACQUIRED EQUIPMENT (CAE)

No CAE is allowed on this TO.

9.2 CONTRACTOR ACQUIRED MATERIAL (CAM)

No CAM is allowed on this TO.

10.0 TRAVEL

For estimating purposes, it is anticipated that the travel requirements noted below shall be required for each performance period. The proposed estimated travel cost cannot exceed the not-to-exceed (NTE) value cited in the applicable pricing model.

# Trips	# People	# Days/Nights	From (Location)	To (Location)
6	3	7/6	Contractor Facilities	Washington D.C.
6	3	7/6	Contractor Facilities	Norfolk, VA
6	3	7/6	Contractor Facilities	San Diego, CA
6	3	7/6	Contractor Facilities	Charleston, SC

11.0 TRANSPORTATION OF EQUIPMENT/MATERIAL

12.0 DELIVERABLES

12.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

12.1.1 Administrative CDRL

As required under TO PWS Para 6.1-6.10, the following table lists all required administrative data deliverables, Contract Data Requirements Lists (CDRLs), applicable to this task:

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
A002	Task Order Status Report	6.9	MTHLY	30 Days after TO award (DATO) and monthly on the 10th
A003	Cyber Security Workforce (CSWF) Report	6.8.15	MTHLY	30 DATO and monthly on the 10th
A004	Contractor Manpower Quarterly Status Report	6.1-6.10	QRTLY	30 DATO and quarterly on the 10th
A005	Task Order Close Out Report	6.1-6.10	1TIME	NLT 15 days before completion date
A006	Contractor Census Report	6.1-6.10	MTHLY	30 DATO and monthly on the 10th
A008	Cost and Schedule Milestone Plan	6.1-6.10	ASREQ	NLT 10 DATO and revisions within 24 hours of request
A009	Contractor CPARS Draft Approval Document (CDAD) Report	6.1-6.10	MTHLY	30 DATO and monthly on the 10th
A016	Invoice Support Documentation	6.9	ASREQ	Within 24 hrs from request

12.1.2 Technical CDRL

The following table lists all required technical data deliverables, Contract Data Requirements Lists (CDRLs), applicable to this task:

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
A007	Quality Documentation	6.9	As Needed	3 Days after Request
A011	Inventory Tracking Report	6.9	Monthly	30 Days after task order (DATO) and monthly on the 10th
A018	Contract Funds Status Report (CFSR)	6.9	Monthly	30 Days after task order (DATO) and monthly on the 10th

CDRL #	Deliverable Title	TO PWS Reference Para	Frequency	Date Due
A021	Technical/Analysis Reports, General	6.8.2,6.8.3,6.8.6,6.8.12,6.8.15, 6.2,6.4,6.8.3	As Needed/ Monthly/ Weekly	30 Days after task order (DATO) and monthly on the 10th

12.2 NON-DATA DELIVERABLES

13.0 SUBCONTRACTING REQUIREMENTS

Subcontracting requirements are in accordance with the basic contract. Note: If a prime contractor plans to utilize subcontractor(s) on this Task Order, the prime must specify in their proposal the intent to utilize subcontractors and list all applicable subcontractor names. Per clause 52.244-2, if a subcontractor is proposed by a prime and is not approved on the basic contract, formal justification is required and subject to government approval.

14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP), Attachment 1.

15.0 OTHER CONDITIONS/REQUIREMENTS

15.1 TO SUPPLEMENTAL PESONNEL QUALIFICATION

15.2 KEY PERSONNEL

Key personnel are those Contractor personnel in positions that the Government considers to be essential to the performance of this Task Order. The Contractor shall notify the COR in writing of any proposed substitution of key personnel at least thirty (30) business days in advance of the proposed action. Such notification shall include explanation of the circumstances necessitating the substitution. The following are considered to be key personnel on this task order: SME 4 and Engineer/Scientist 4.

15.3 CYBER SECURITY WORKFORCE DESIGNATION

All cyber security workforce personnel working on this task order are required to hold valid cybersecurity baseline credentials.

16.0 LIST OF ATTACHMENTS

Attachment 1 – Quality Assurance Surveillance Plan (QASP)

SECTION D PACKAGING AND MARKING

All Deliverables shall be packaged and marked IAW Best Commercial Practice.

SECTION E INSPECTION AND ACCEPTANCE

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
2001	Destination	Government	Destination	Government
2006	Destination	Government	Destination	Government
3001	Destination	Government	Destination	Government
3006	Destination	Government	Destination	Government
4001	Destination	Government	Destination	Government
4006	Destination	Government	Destination	Government

SECTION F DELIVERABLES OR PERFORMANCE

The periods of performance for the following Items are as follows:

2001 9/28/2015 - 9/27/2016

2004 Same as CLIN 2001

3001 365 days from the date CLIN 3001 is exercised
3004 Same as CLIN 3001

4001 365 days from the date CLIN 4001 is exercised
4004 Same as CLIN 4001

SECTION G CONTRACT ADMINISTRATION DATA

The SPAWAR Atlantic Ombudsman is Steven G. Harnig, (843) 218-4560.

THIS IS A COST PLUS FIXED FEE, LEVEL OF EFFORT TYPE ORDER.

The number of hours estimated for this LOE tasking is (b)(4) standard hours. In performing the requirements of this order, the contractor may use any combination of hours from the labor categories approved at the basic contract level, so long as the estimated total cost and the funded amount to date for the order is not exceeded and the total number of hours provided does not exceed the estimated number of hours by more than 5%.

5252.232.9400 LIMITATION OF LIABILITY- INCREMENTAL FUNDING (JAN 1992)

This TASK order is incrementally funded and the amount currently available for payment hereunder is limited to $5,040,972.07 inclusive of fee. It is estimated that these funds will cover the cost of performance through 27 Sept 2016. Subject to the provision of the clause entitled Limitation of Funds (FAR 52.232-22) of the general provisions of this contract, no legal liability on the part of the Government for payment in excess of $5,040,972.07 shall arise unless additional funds are made available and are incorporated as a modification to the TASK order.

Estimated CPFF Total Order NTE*	Total Funded Amount	Unfunded Amount
$10,059,780.40	$5,040,972.07	$5,018,808.33

The contractor shall cite on each invoice/voucher, in addition to all other requirements of this contract/order, the contract line item number (CLIN); the contract subline item number (SLIN) and accounting classification reference number (ACRN) for the portion, or portions of work being billed as specified in the contract or delivery order. For each ACRN on the invoice/voucher, the contractor shall identify the amount being billed against that ACRN.

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (JUN 2012)

(a) Definitions. As used in this clause--

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.
(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the Central Contractor Registration at https://www.acquisition.gov; and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this Web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at https://wawf.eb.mil/.
(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) *WAWF payment instructions*. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) *Document type*. The Contractor shall use the following document type(s).

Cost Type Orders - Cost Voucher

(2) *Inspection/acceptance location.* The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

N65236

(3) *Document routing*. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table

**Field Name in WAWF*	*Data to be entered in WAWF*
Pay Official DoDAAC	*DFAS HQ0338
Issue By DoDAAC	N65236
Admin DoDAAC	*DCMA S2404A

Inspect By DoDAAC	N65236
Ship To Code	*
Ship From Code	*
Mark For Code	*
Service Approver (DoDAAC)	*
Service Acceptor (DoDAAC)	*
Accept at Other DoDAAC	
LPO DoDAAC*****	
DCAA Auditor DoDAAC	HAA031
Other DoDAAC(s)	

	Cost Type Orders	**Fixed Price Orders**
WAWF Invoice Type	Cost Voucher	2-N-1 (Services Only)
Issuing Office DODAAC	N65236	N65236
Admin DODAAC:	*DCMA S2404A	*DCMA
Inspector DODAAC (if applicable)	N65236	N65236
Acceptor DODAAC:	N65236	N65236
LPO DODAAC:		
DCAA Auditor DoDAAC:	*DCAA HAA031	*DCAA
Service Approver DoDAAC:	*	*
PAY DODAAC:	*DFAS HQ0338	*DFAS

252.204-0002 Line Item Specific: Sequential ACRN Order. (SEP 2009)

The payment office shall make payment in sequential ACRN order within the line item, exhausting all funds in the previous ACRN before paying from the next ACRN using the following sequential order: Alpha/Alpha; Alpha/numeric; numeric/alpha; and numeric/numeric.

```
Accounting Data

SLINID   PR Number                                          Amount
-------- -------------------------------------------------- ---------------------
200101   130052703900005                                    2806000.00
LLA :
AA 1751804 KT1M 257 00025 1 068732 2D 5RC146 AA000271CIOP
Standard Number: N0002515RC00146
NWA - 100001083504-0010

200102   130052703900007                                    2234972.07
LLA :
AB 1751804 KT1M 257 00025 1 068732 2D 5RC147 AA000271CIOP
Standard Number: N0002515RC00147
NWA-100001083503-0020


BASE Funding 5040972.07
Cumulative Funding 5040972.07
```

SECTION I CONTRACT CLAUSES

252.239-7001 **Information Assurance Contractor Training and Certification.**

Information Assurance Contractor Training and Certification (JAN 2008)(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

Code of Federal Regulations / Title 48 - Federal Acquisition Regulations System / Vol. 3 / 2008-10-01462
(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

SECTION J LIST OF ATTACHMENTS

Attachment 1 - QASP